

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF GEORGIA  
AUGUSTA DIVISION

UNITED STATES OF AMERICA )  
 )  
v. ) INDICTMENT NO. CR 109-074  
 )  
REGINALD LONNEL CRAY, )  
 )  
Defendant. )

**GOVERNMENT’S RESPONSE TO**  
**DEFENDANT’S MOTION TO SUPPRESS**

Now comes the United States of America, by and through Edmund A. Booth, Jr., United States Attorney for the Southern District of Georgia, and the undersigned Assistant United States Attorney, and responds to Defendant's Motion to Suppress Search of 3686 Red Leaf Way, Martinez, Georgia and Evidence Obtained Pursuant Thereto, as follows:

## I. Investigation and Search Warrant Information

1. In late 2005, through an investigation named Operation Emissary, United States Immigration and Customs Enforcement (ICE) agents began an investigation into the operators of and subscribers to hard-core child pornography websites available worldwide over the Internet. The success of that investigation, which has resulted in more than 300 domestic convictions of website subscribers spanning approximately 40 states, and including dozens of convicted sex offenders and child molesters, later led to a similar investigation, dubbed Operation Thin Ice.<sup>1</sup>

2. As described more fully in the Search Warrant Affidavit beginning at paragraph 27, during Operation Thin Ice, ICE investigators were able to identify by name, address, e-mail account,

<sup>1</sup> The details of Operation Emissary and Operation Thin Ice are provided in the Search Warrant affidavit filed under seal with case number 1:09-MJ-18, issued April 23, 2009.

password, login, and credit card number those individuals who subscribed to a particular hard core child pornography website under investigation (hereafter “Website” or “Child Pornography Website”), as that information had been provided by the potential subscriber to the operator of the Website in order to gain access to the Child Pornography Website. In addition, ICE agents could identify the IP address from which a subscription was made, and the URL of the child pornography advertising website through which the subscription purchase occurred.

3. In March 2008, as part of its investigation, ICE, tasked with policing the unlawful importation of prohibited items, including child pornography, identified thousands of images and videos containing child pornography on the Child Pornography Website. A detailed description of a sampling of those images is included in the Search Warrant Affidavit at paragraph 41, including files with names that include the country names of “asia” and “brasil.”<sup>2</sup>

4. Between May and July 2008, a search of the server which hosted the Child Pornography Website revealed thousands of images and videos of child pornography, as well as log files which identified by email address, subscriber information and IP address, individuals who had accessed the Child Pornography Website between October 2007 and June 2008. This information coupled with subscriber information earlier obtained, allowed ICE agents to match website subscribers to the actual child pornography images they had accessed and the time of that access.

5. In so doing, ICE was able to determine that Defendant Cray subscribed to the Child Pornography Website on March 25, 2008, using a certain email address and credit card, and

---

<sup>2</sup> In addition, when ICE attempted to match the child pornography images at issue in this case with previously identified images (commonly referred to as “known images”) through a national database of known victims, the ICE agent found that several of the images possessed by Defendant Cray depicted minors from other countries, including Poland and the United Kingdom.

accessing the website through an identified IP Address and email account. On that same date, using commercially available software, ICE agents were able to determine that the IP address at issue was controlled by AT&T Internet Services Southeast. And in response to a Customs Summons issued by ICE under the authority of 19 U.S.C. § 1509, on March 27, 2008, AT&T, Inc. related, among other things, that the geographical address for the subject IP Address was 4686 Red Leaf Way, Martinez, Georgia.<sup>3</sup>

6. In addition, ICE was able to determine, based on evidence gathered following the execution of search warrants on a particular email address connected to the Website's subscription process, that on March 25, 2008, the email address used by Cray received an instructional email about how to access the Child Pornography Website. Further, the log file evidence obtained during the search of the server in May and July 2008 (mentioned above), revealed that on March 25, 2008, a person at the IP address associated with Cray's residence accessed the Child Pornography Website. Moreover, the email address associated with Cray's subscription, was shown to have accessed numerous child pornography images between March 25, 2008 and April 14, 2008. Notably, several of those images fully described in the Search Warrant Affidavit at paragraph 54, had the country name of "asia" contained within the file name of the images. (See also, footnote 2)

---

<sup>3</sup> The Customs Summons issued to AT&T, Inc. on March 27, 2008, requested the name, address, telephone number, billing records, additional screen names, email accounts, and any other subscriber information including length of service, start date and types of services utilized, connection records including dates and times, all available IP history logs and method of payment for following the IP address (listing the IP address) from March 24, 2008 to March 26, 2008. However the only information included in the Search Warrant Affidavit which was obtained from AT&T in response to this Customs Summons was the address of the Subject Premises. (See Search Warrant Affidavit at paragraph 51.)

7. The above-cited information provided the necessary probable cause to believe Cray, or someone at his residence, had subscribed to and viewed images on the Child Pornography Website between March 25, 2008 and April 14, 2008. However, additional information was included in the Search Warrant Affidavit, confirming that the Defendant continued to reside at the subject address in or around April 2009, when the subject search warrant was sought.

8. Specifically, in conjunction with ICE's continuing investigation of Cray's possession and receipt of child pornography, ICE issued a Customs Summons to Georgia Power on February 6, 2009, requesting the subscriber information associated with Reginald Cray at the subject address. In response, Georgia Power relayed information that an Olivia Cray had a Georgia Power account at the subject address, and said information was included in the Search Warrant Affidavit at paragraph 56.

9. ICE also issued a Customs Summons on February 12, 2009, to AT&T Southeast, requesting subscriber and associated information relating to the address, name, account number, email address, phone number, service status and log-in times from January 15 to the date of the summons, for Reginald and Olivia Cray, at the Red Leaf address. The only information received from AT&T in response to this Summons which was included in the Search Warrant Affidavit was confirmation that the subject phone number (provided by ICE to AT&T) was subscribed to Reginald Cray at the subject address.<sup>4</sup>

---

<sup>4</sup> An even more precise address confirmation was obtained – without the use of a Customs Summons – from the Post Master in April 2009, when the Post Master confirmed the receipt of mail by Reginald Cray at the subject address, (See Affidavit at paragraph 57,) rendering the other address-confirming paragraphs cumulative and unnecessary.

10. Finally, ICE issued a Customs Summons on March 3, 2009, to First National Bank (FBN South) requesting Cray's bank statements for March and April 2008 transaction of 79.99 to a particular merchant account from Cray, and providing the specific credit account number at issue. Based on FBN South's response to the Summons, in the Search Warrant Affidavit the affiant related the confirmation by the bank that Cray had the subject credit card issued to him at a Fort Gordon Post Office Box, and that a 79.99 charge was made to that account from the merchant account associated with the Child Pornography Website. Notably, even without this confirmation, ICE agents had probable cause to believe Cray had purchased the subscription, given the information they had obtained in March 2008, described in paragraph 5 above.

11. Based on all the information contained in the Search Warrant Affidavit, only some of which has been recited herein, on April 23, 2009, finding probable cause to support the same, this Court issued a Search Warrant for the subject premises. That warrant was executed by federal and state agents on April 28, 2009. During the search, Cray, who was not in custody and had been informed by agents that he was free to decline answering questions, agreed to be interviewed. Thereafter, Cray made admissions related to the charged offenses.

12. Further, a forensic examination of the computers seized from Cray's residence revealed a registry log depicting numerous images and videos from the Child Pornography Website which Cray received and possessed while he was a subscriber to the Website. The instant Indictment charging Receipt and Possession of Child Pornography followed.

13. Defendant now files this Motion to Suppress the evidence obtained from his residence claiming that the ICE agents improperly used Customs Summonses to obtain banking and account information to establish probable cause, rather than using a process under the Right to Financial

Privacy Act of 1978 at 12 U.S.C. 3401 et seq. and Access to Stored Communications Act, 18 U.S.C. 2701 et seq. Defendant's motion, which is unsupported by authority, and is without merit, should be denied.

## **II. Cray Lacks Standing to Challenge Evidence Obtained Through Customs Summons**

14. As a preliminary matter, because Cray has asserted neither a subjective nor an objectively reasonable expectation of privacy in the information provided to ICE pursuant to the Customs Summonses, he has no standing to challenge that information's release and use. See *Katz v. United States*, 389 U.S. 347, 353 (1967) (holding that "the capacity to invoke the protection of the Fourth Amendment depends . . . on whether the person seeking the protection of the amendment had a legitimate expectation of privacy in the invaded place.") (Harlan, J., concurring). In his motion, Defendant made no attempt to assert a subjective privacy expectation in the information obtained through the Customs Summons, nor has he explained why such an expectation, if so held by the defendant, is one that society is prepared to accept. *Id.*

15. Notably, other than address and account confirming information gained from the Customs Summonses, the only other information received by way of a Customs Summons to support a probable cause finding for the search warrant was subscriber information and a residence address received from Cray's service provider, AT&T Southeast and bank records verifying an earlier transactions. Yet federal courts have consistently held that such information is not protected by the Fourth Amendment. See *United States v. Perrine*, 518 F.3d 1196, 1204 (10<sup>th</sup> Cir. 2008) (holding that "subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.") (citations omitted.); *United States v. Miller*, 425 U.S. 435, 443

(1976) (holding that account holders lack standing to challenge subpoenas to banks as bank records are business records to which the defendant has no expectation of privacy.)<sup>5</sup>

16. Absent a showing of standing, the Defendant's motion should be denied outright.

### **III. Customs Summons Properly Used As Investigative Tool**

17. Even if this Court were to find that the defendant has standing to challenge the issuance of the Customs Summonses for the requested information, the law supports the use of Customs Summonses here.

18. A Customs Summons is authorized under section 509 of the Tariff Act of 1930, codified at 19 U.S.C. § 1509. 19 U.S.C. § 1509, in relevant part, provides:

(a) Authority

In any investigation or inquiry conducted for the purpose of . . . insuring compliance with the laws of the United States administered by the United States Customs Service, the Secretary (but no delegate of the Secretary below the rank of district director or special agent in charge) may—

(2) summon, upon reasonable notice--

(A) the person who—

(I) imported, or knowingly caused to be imported, merchandise into the customs territory of the United States, ...

(B) any officer, employee, or agent of any person described in subparagraph (A);

(C) any person having possession, custody or care of records *relating to the importation or other activity described in subparagraph (A)*; or

(D) *any other person he may deem proper*;

to appear before the appropriate customs officer at the time and place within the customs territory of the United States specified in the summons . . . to produce records, as defined in subsection (d)(1)(A) of this section, and to give such testimony, under oath, *as may be relevant to such investigation or inquiry*.

---

<sup>5</sup> Notably, although the Right to Financial Privacy Act was passed into law after this holding, its enactment does not change the Fourth Amendment jurisprudence on the issue, which requires a defendant to show that he had a legitimate expectation of privacy in the information obtained.

(d) Special procedures for third-party summonses

(1) For purposes of this subsection–

(A) The term “records” includes those--

...

(ii) regarding which there is probable cause to believe that *they pertain to merchandise the importation of which into the United States is prohibited.*

19 U.S.C. § 1509 (emphasis added).

19. Although in its full reading the summons-related authority may appear to focus primarily on regulating the import and export of merchandise, it also covers other federal laws regulated by ICE, including child pornography laws. ICE enforces the child pornography laws, in part, because child pornography was historically manufactured elsewhere, and then imported into the United States. See e.g. *Hallock v. United States*, 253 F.Supp. 2d 361, 365 (N.D.N.Y. 2003)(recognizing that “customs officers have been traditionally responsible for investigating wrongdoing on a national and even global stage” to include the investigation of purveyors of child pornography.) Through the use of the Internet, the distribution of child pornography has no geographic limits, and the Customs Service, now ICE, has regularly used its summons authority under 19 U.S.C. § 1509 to obtain subscriber information on Internet accounts. See e.g. *United States v. Hamilton*, 413 F.3d 1138, 1141 (10<sup>th</sup> Cir. 2005).

20. As outlined in the statute, a Customs Summons may be issued upon any person deemed proper, if the records that person maintains may be relevant to an investigation of the importation of items into the United States. Here, ICE properly utilized the subject Customs Summonses to gather documents and information relevant to an investigation of the likely importation of child pornography images which (1) had file names with the country names of “asia” and “brasil” in them; and (2) depicted child victims from Poland, the United Kingdom, and elsewhere. Through



the summoned information, ICE agents were able to initially locate the residence address associated with the IP address of the Defendant, and later verify Cray's continued presence at that address at or near the time of the search warrant's execution. Agents were also able to verify the credit card transaction which facilitated the Defendant's purchase of a subscription to the Child Pornography Website.

21. Contrary to Defendant's assertion, and as evidenced above by the plain language of the statute, the use of a third-party summons is not limited to customs brokers, attorneys and accountants. Although the statute expressly list those groups of individuals at 19 U.S.C. § 1509(d)(1)(C) as potential recipients, it does so in defining the term "third party recordkeepers" and setting forth a notice requirement – not at issue here.

22. Therefore, because the Customs Summonses were properly used in this case to further a legitimate investigative purpose, the information derived therefrom and used to support the probable cause finding related to the subject search warrant is not subject to suppression and Defendant's motion should be denied.

#### **IV. Right to Financial Privacy Act Permits Customs Summons**

23. Likewise, the Right to Financial Privacy Act of 1978, codified at 12 U.S.C. § 3401 et seq., allows for the use of Customs Summons in the circumstances found here.

12 U.S.C. § 3402 provides in relevant part:

Except as provided by section 3403(c) or (d), 3413, or 3414 of this title, no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and--

...

2) such financial records are disclosed in response to an administrative subpoena or *summons* which meets the requirements of section 3405 of this title;

(Emphasis added). 12 U.S.C. § 3405 regarding administrative subpoenas and summons, provides in relevant part:

A Government authority may obtain financial records under section 3402(2) of this title pursuant to an administrative subpoena [sic] or summons otherwise authorized by law only if–

(1) there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry;

(2) a copy of the subpoena or summons has been served upon the customer or mailed to his last known address on or before the date on which the subpoena or *summons* was served on the financial institution together with the following notice which shall state with reasonable specificity the nature of the law enforcement inquiry . . .

(Emphasis added).

However, 12 U.S.C. § 3413(g), provides the following exception to the notice requirement:

(g) Disclosure pursuant to legitimate law enforcement inquiry respecting name, address, account number, and type of account of particular customers

The notice requirements of this chapter and sections 3410 and 3412 of this title shall not apply when a Government authority by a means described in section 3402 of this title and for a legitimate law enforcement inquiry is seeking only the name, address, account number, and type of account of any customer or ascertainable group of customers associated (1) with a financial transaction or class of financial transactions . . . .

24. Here the only Customs Summons that has any relation to the Financial Privacy Act is the one issued to First National Bank (FNB South). Through that summons ICE requested “all subscriber and associated information relating to the following address, name, account number, Bank statements for March and April, transaction of 79.99 to [merchant account] from Reginald Cray 10/28/08 credit/debit account [number provided].” Notably, the information sought was intended to further a legitimate investigation and to verify the credit card and transaction information related to Cray’s purchase of a subscription to the Child Pornography Website which ICE had

obtained in March 2008. The request did not actually seek the name, address, or account number of Cray, but instead merely sought to verify through a bank statement specific transaction information already available to ICE. Because the information requested was limited in scope to verify account information about a specific transaction, in accordance with the statute's exception, no notice was provided to Cray with regard to that Summons.<sup>6</sup> See 12 U.S.C. § 3413(g).

25. Even if this Court were to find that ICE violated the requirements of the Financial Privacy Act when issuing the Customs Summons without providing notice to Defendant, because the information obtained and included in the Search Warrant Affidavit was cumulative with regard to the purchase of a subscription to the Child Pornography Website, it does not undermine the probable cause finding by this Court in support of the subject search warrant.

26. Further, because any violation of the Financial Privacy Act does not arise as a Fourth Amendment violation, requiring the suppression of evidence, Defendant's motion should be denied.

#### **V. Electronic Communications Privacy Act of 1986 Permits Use of Customs Summons**

27. Similarly, the Electronic Communications Privacy Act of 1986, codified at 18 U.S.C. § 2701 et seq. permits the use of a Customs Summons, without notice to the customer, in the circumstances found here.

Specifically, 18 U.S.C. §§ 2703(c) provides in relevant part:

(c) Records concerning electronic communication service or remote computing service.--

---

<sup>6</sup> Notably, the information received from FNB South exceeded that of the request in that FNB South included bank statements for March, April and May of 2008, when only the April bank statement reflected the transaction in question. Despite receiving more information than requested, ICE only included in its Search Warrant Affidavit the specific information requested from the bank: confirmation of the subscription purchase transaction; rendering any overage in production irrelevant to this analysis.

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

...

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

28. Because the Customs Summons issued in the instant case to AT&T, Inc., (Cray's internet service provider) did not exceed the parameters set forth by the statutory provision outlined above, the evidence obtained therefrom could be used by this Court to find probable cause in support of the subject search warrant.

29. Notably, even if this Court were to find that the information obtained exceeded that permitted by the ECPA, the remedy available to the defendant is not suppression of that evidence, but a civil action for damages. *See United States v. Sherr*, 400 F.Supp.2d 843, 848 (D. Md. 2005);

see also *United States v. Kennedy*, 81 F.Supp.2d 1103, 1110 (D.Kan. 2000) (holding that “Congress clearly intended for suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of ECPA.”)

## **VI. *Leon* Good Faith Exception**

30. Even if this Court were to find (1) that Cray had a reasonable privacy expectation in the information ICE obtained through the Customs Summons; (2) that the Customs Summonses were so infirm as to require excising the related information from the Search Warrant Affidavit; *and* (3) that as a result the excision of that information the Court had insufficient facts upon which to find probable cause to support the subject search warrant, (none of which the government concedes) because the law enforcement officers acted with the objectively reasonable belief that their conduct did not violate the Fourth Amendment, exclusion of the seized evidence would be inappropriate. *See United States v. Leon*, 468 U.S. 897, 917, 104 S.Ct. 3405 (1984).

31. The Supreme Court in *Leon*, clearly established that the purpose of the exclusionary rule is to prevent police misconduct, not to vindicate the privacy rights of a defendant. *Leon*, 468 U.S. at 906, 104 S.Ct. at 3412. Accordingly, absent an allegation that the magistrate abandoned his detached and neutral role – which has not been made here – suppression of evidence would only be appropriate if Defendant could show that ICE S.A. McManaway was dishonest or reckless in preparing his affidavit, or could not have had an objectively reasonable belief in the existence of probable cause. *See Leon*, 468 U.S. at 925. Neither situation has been alleged or exists here.

32. First, though the Defendant alleges that the ICE agents relied upon the wrong statute and subpoena process to pursue evidence in this case, he does not allege dishonest or reckless behavior by the agents, and none is evident. Further, S.A. McManaway, and the other ICE agents involved

in this investigation, could reasonably believe, based on the common use of Customs Summons to obtain the kind of information requested here, that the information was properly obtained and that probable cause existed to search Cray's residence and computers.

33. Therefore, even if the court finds the warrant for Cray's residence and computers invalid, the evidence should not be suppressed as it was obtained pursuant to a search warrant that the officers could reasonably and in good faith rely upon.

### **VII. Conclusion**

For the foregoing reasons, Defendant's Motion to Suppress is without merit, and should be denied.

Respectfully submitted, this 7<sup>th</sup> day of August, 2009.

EDMUND A. BOOTH, JR.  
UNITED STATES ATTORNEY

*/s/ Nancy C. Greenwood*

---

Nancy C. Greenwood  
Assistant United States Attorney  
Georgia Bar No. 309179  
Post Office Box 2017  
Augusta, Georgia 30903  
(706) 826-4520

**CERTIFICATE OF SERVICE**

This is to certify that I have this 7<sup>th</sup> day of August 2009, served counsel in this case with a copy of the foregoing either by electronic filing notification or by depositing a copy of the same in the United States mail in a postpaid envelope, properly addressed to:

John T. Garcia  
205-B N. Belair Road  
P.O. Box 1984  
Evans, GA 30809

*/s/ Nancy C. Greenwood*

---

Nancy C. Greenwood  
Assistant United States Attorney